IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	§	Attorney Docket No. **AUS920030659US1**
CHEN, ET AL.	§	
	§	
Serial No.: **10/692,127**	§	Examiner: **ALAN S. CHOU**
	§	
Filed: **10/23/2003**	§	
	§	
For: **ENHANCED DATA SECURITY**	§	Art Unit: **2151**
THROUGH FILE ACCESS CONTROL OF	§	
PROCESSES IN A DATA PROCESSING	§	
SYSTEM	§	

APPEAL BRIEF UNDER 37 C.F.R. 41.37

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

     This Brief is submitted in support of the Appeal of the Examiner's final rejection of Claims 1-24 in the above-identified application. A Notice of Appeal was filed in this case and received in the Patent Office on May 3, 2008. A one month extension of time is required to file the Brief, and is hereby requested. Please charge the fee of $120.00 for the extension of time to **DILLON & YUDELL LLP's Deposit Account No. 50-3083**. Please charge the fee of $510.00 due under 37 C.F.R. §1.17(c) for filing the brief, as well as any additional required fees, to **IBM's Deposit Account No. 09-0447.**

REAL PARTY IN INTEREST

The real party in interest in the present Application is International Business Machines Corporation, the Assignee of the present application as evidenced by the Assignment set forth at reel 014642, frame 0823.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, the Appellants' legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-24 stand finally rejected by the Examiner as noted in the Final Office Action dated December 5, 2007. The rejection of Claims 1-24 is appealed.

STATUS OF AMENDMENTS

No amendment to the claims was made in the Appellants' Response A, filed on September 24, 2007, and no amendment was made subsequent to the Final Action from which this appeal is taken.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellants' Claim 1 provides a method (FIG. 8) in a data processing system (FIG. 1) for controlling the transfer of data from the data processing system to a network 151 (FIG. 1). The method comprises the steps of: creating a file list (302, FIG. 3A) of one or more data files to be controlled (806, FIG. 8; ¶0051); creating a process list (310, FIG. 3B) for each data file in the file list (302), wherein each process list (310) identifies one or more processes executing in the data processing system that has accessed the data file associated with the created process list (FIG. 5; ¶0048); receiving a request from a requesting process executing in the data processing system to transfer data from the data processing system to the network (802, FIG. 8; ¶0051); determining if the requesting process is identified in one or more created process lists (804, FIG. 8; ¶0051); and if the requesting process is identified in a created process list (310), prohibiting the requested transfer of data from the data processing system to the network (806, FIG. 8; ¶0051).

Appellants' invention also provides at Claim 9, a data processing system (FIG. 1) for controlling the transfer of data from a data processing system (FIG. 1) to a network (151) comprising: means for (processing unit 121, FIG. 1; process manager 230, FIG. 2; etc.) creating a file list (302, FIG. 3A) of one or more data files to be controlled (806, FIG. 8; ¶0051); means for creating a process list (310, FIG. 3B) for each data file in the file list (302), wherein each process list (310) identifies one or more processes executing in the data processing system that has accessed the data file associated with the created process list (FIG. 5; ¶0048); means for receiving a request from a requesting process executing in the data processing system to transfer data from the data processing system to the network (802, FIG. 8; ¶0051); means for determining if the requesting process is identified in one or more created process lists (804, FIG. 8; ¶0051); and means for, if the requesting process is identified in a created process list (310), prohibiting the requested transfer of data from the data processing system to the network (806, FIG. 8; ¶0051).

Appellants' Claim 17 provides an article of manufacture (e.g., 129, 131, FIG. 1) comprising machine-readable medium (id.) including program logic embedded therein (see ¶0052) that causes control circuitry in a data processing system (e.g., FIG. 1) for controlling the transfer of data from a data processing system (FIG. 1) to a network (151) to perform the above described method steps (FIG. 8).

Other features recited by Applicants' claimed invention include: wherein the step of creating a process list includes adding a first process to a process list when the first process receives data from a second process identified on the process list (Claim 2, 10, 18; 604, 606, FIG. 6; ¶0049); wherein the first process is only added to the process list when the received data is related to the process list's associated data file (Claim 3, 11, 19; 606, FIG. 6; ¶0049); wherein the step of receiving includes receiving a request from a requesting process executing in the data processing system to transfer a data file listed in the file list from the data processing system to the network (Claim 4, 12, 20; 802, FIG. 8; ¶0051). In one embodiment, the method further comprises the step of requesting authorization to perform the requested transfer of data from the data processing system to the network (Claim 5, 13, 21; 810, FIG. 8; ¶0051); wherein the step of

requesting includes sending a message to a user of the data processing system displayed in a graphical user interface (Claim 6, 14, 22; 806, FIG. 8; ¶0051). The method further comprises the step of performing the prohibited transfer of data from the data processing system to the network upon receipt of authorization to make the transfer of data (Claim 7, 15, 23; 808, FIG. 8; ¶0051). Finally, the method comprises wherein the authorization is a command received from a user of the data processing system (Claim 8, 16, 24; FIG. 8; ¶0051).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A.   The Examiner's rejection of Claims 1-4, 9-12 and 17-20 under 35 U.S.C. §102(b) as being anticipated by *Oe et al.* (U.S. Patent Publication No. 2002/0099837) (hereinafter *Oe*) is to be reviewed on Appeal.

B.   The Examiner's rejection of Claims 5-8, 13 and 21 under 35 U.S.C. §103(a) as being unpatentable over *Oe* in view of *Yamaguchi et al.* (U.S. Patent Publication No. 2004/0064572) (hereinafter *Yamaguchi*) is to be reviewed on Appeal.

ARGUMENT

A.   The rejection of Claims 1-4, 9-12 and 17-20 under 35 U.S.C. §102(b) as being anticipated by *Oe et al.* (U.S. Patent Publication No. 2002/0099837) is not well founded and should be reversed.

A.1 General requirements for a claim rejection under 35 U.S.C. §102

The applicable statutory language for 35 U.S.C. §102(b) provides that:

A person shall be entitled to a patent unless --

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

The interpretation/meaning of that statutory standard is further provided by case law, which indicates that anticipation is established only when a single prior art reference discloses, expressly or under the principles of inherency, each and every element of a claimed invention as well as disclosing structure which is capable of performing the recited functional limitations.

RCA Corp. v. Applied Digital Data Systems, Inc., 730 F.2d 1440, 221 USPQ 385 (Fed. Cir. 1984); *W.L. Gore and Associates, Inc., v. Garlock. Inc.,* 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983).

A.2 *Oe* does not teach each and every element of Example Claim 1

Oe fails to anticipate Appellants' claimed invention because *Oe* does not teach or suggest each and every feature recited by Appellants' independent claims. Specifically, *Oe* does not teach or suggest the following elements and corresponding features of Appellants' example independent Claim 1 (and/or independent Claims 9 and 17, which provide similarly constructed elements):

> (1) *creating a process list* for each data file in the file list, wherein each process list *identifies* one or more *processes* executing in the data processing system *that has accessed the data file* associated with the created process list;

> (2) *receiving a request* from a requesting process executing in the data processing system to *transfer data* from the data processing system *to the network;*

> (3) determining if the *requesting process* is *identified in* one or more created *process lists;* and

> (4) if the requesting process is identified in a created process list, *prohibiting the requested transfer of data* from the data processing system *to the network.*

(Example Claim 1; underlining added for emphases).

As provided by the preamble to the above claim elements, Appellants' invention provides a "method in a data processing system for controlling the transfer of data from the data processing system to a network." Applicants' invention addresses security issues relating to transferring data from the data processing system onto the network. Each of the above claim features are then directed to enabling completion of the method steps that achieve this stated objective.

In contrast to the teachings of Applicants' claimed invention, *Oe* provides a computer resource access control technique having a "trap" feature in which a resource request is trapped pending the outcome of an access determination (*see* Abstract, page 1 and ¶¶ 0009 - 0013). As

recited at ¶ 0009, *Oe* provides: "an information processing method of controlling access to computer resource(s) managed by an operating system, such as a file, network, storage device, display screen, or external device." Page 1, ¶ 0015 describes an "access right management table" containing resource designation information that designates a specific computer resource, condition information under which the access right is validated, and access right information that designates an access right. *Oe* as a whole does not teach the features of Appellants' invention, and the cited sections of *Oe* relied upon by Examiner to support the rejections of specific features of Appellants' claim elements also fail to teach or suggest those claim features.

For example, *Oe* does not teach the "creating a process list ..." feature(s) of Appellants' example claim. In contrast, the section of *Oe* referenced by Examiner as teaching this feature, namely page 9, section 0224 provides: "[t]he condition 20352 represents a condition or a combination of conditions under which the access right is validated. For example, a user name/ID, group name/ID, time, application limited for use, and the like are registered." This recitation does not teach or suggest the creating a process list features of Appellants' example claim.

As another example, *Oe* also does not teach the "receiving a request ... to transfer data ... to the network" feature(s) of Appellants example claim. The referenced section of *Oe*, page 1, sections 0009 and 0010 describes a trap step of trapping an operation request from a process or operating system for the computer resource before granting access to the computer resource. These sections are, however, devoid of any teaching or suggestion of receiving a request to transfer data to the network, as recited by Appellants' claims.

Additionally, page 1, section 0011 of *Oe* does not teach the "determining if the requesting process is identified in one or more created process lists" feature(s) of Appellants' claims. Rather, that section describes a determination of "whether an access right for the computer resource designated by the operation request trapped in the trap step is present." There is no mention or suggestion of determining whether a requesting processing is contained in a "process list", which list is created/used in accordance with the above-mentioned claim elements.

Finally, page 1, section 0013 of *Oe* recites: "a denial step of denying the operation request if it is determined in the determination step that no access right is present." However, denying an operation if no access right is present does not anticipate (i.e., fails to teach or suggest) "if the requesting process is identified in a created process list, prohibiting the requested transfer of data from the data processing system to the network," as recited by Appellants' Claim 1. *Oe*'s system only references localized access to a resource on the single computer device, with no teaching or suggestion of a data transfer to the network.

For the above stated reasons, *Oe* fails to teach or suggest several of the features recited by Appellants' example Claim 1 and by extension independent Claims 9 and 17 and the respective dependent claims. The standard for determining a §102 anticipation rejection requires that the reference teach each and every element recited in the claims. *Oe* fails to meet this standard and, therefore, *Oe* does not anticipate Appellants' claims. Appellants' claims are therefore allowable. Appellants respectfully request the Board reverse the Examiner's rejection of Appellants' claims.

B.   The rejection of Claims 5-8, 13 and 21 under 35 U.S.C. §103(a) as being unpatentable over *Oe* in view of *Yamaguchi et al.* is not well founded and should be reversed.

B. 1 General requirements for a claim rejection under 35 U.S.C. § 103

According to 35 U.S.C. §103(a):

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

In order to make the obviousness determination, the U.S. Supreme Court held in Graham v. John Deere Co., 383 U.S. 1 (1966) (hereinafter *John Deere*) that three factors must be considered:

(1)   the scope and content of the pertinent prior art;
(2)   differences between the pertinent prior art and the invention at issue; and
(3)   the ordinary level of skill in the pertinent art.

In *KSR Intern. Co. v. Teleflex, Inc.*, 127 S.Ct. 1727 (2007), the U.S. Supreme Court clarified that a non-obviousness determination must include an inquiry as to "whether the improvement is more than the predictable use of prior art elements according to their established functions."

First, the present claims are dependent on the independent claims (1, 9, and 17), which Appellants have shown to be allowable over the primary reference (*Oe*). Given their dependence on allowable base claims, the present claims are also allowable. Appellants however also address below the deficiencies found in the references and combination thereof with respect to the *John Deere* factors, on the one hand, and the claim features, on the other hand.

Example dependent claims 5-7, respectively recite "requesting authorization to perform the requested transfer of data from the data processing system to the network;" (Claim 5) "wherein the step of requesting includes sending a message to a user of the data processing system displayed in a graphical user interface" (Claim 6); and "performing the prohibited transfer of data from the data processing system to the network upon receipt of authorization to make the transfer of data" (Claim 7). Neither reference teaches these features. The combination of the references also fails to teach or suggest these features, and one skilled in the art would not find these features to be suggested by the combination.

In analyzing the above claims (and with reference to example claims 5-7), Appellants point to the clear failure of the combination to pass the first two of the above *John Deere* factors, and Appellants respectfully traverse the 103 rejection for failing to pass these factors. As laid out in the arguments traversing the 102 rejections, the primary reference *Oe* does not teach or suggest many of the features recited by example Claim 1, from which Claims 5-7 depend. Further, as alluded to above, *Oe* is concerned about a different problem and describes a different process that yields a very different result from Appellants' claims. Additionally, and as explained above, given the significant differences between *Oe*'s disclosure and Appellants' recited claim elements, one skilled in the art would not find Appellants' claims to be suggested by *Oe*'s disclosure. Thus, the scope and content of *Oe*'s disclosure does not suggest the specific features of Appellants' claims.

Yamaguchi fails to make up for these deficiencies in *Oe*, and is only provided to support the rejection of the present dependent claim features. The specific section of *Yamaguchi* provided to reject the features, namely page 3, section 0062, provides:

> *In a case where the authorization level is protect, as mentioned above (if the authorization level is private, data such as a service name is not stored in the service list and, hence, a private service name, etc., cannot be selected from the service list), authentication processing is necessary. The authentication processing makes use of a GUID that corresponds to the service and that has been encrypted, as will be described later. This means that in a case where a service name, etc., is transmitted, a GUID that corresponds to the service name, etc., transmitted and that has been encrypted is also transmitted from the client computer 1 to the service server 2.*

However, transferring a global user id (GUID) during authentication processing from the client computer to the server does not teach or suggest the features recited by the example Claims 5-7. There is no teaching or suggestion within *Yamaguchi* of the features recited by Appellants' example claims. Appellants' claims clearly provide more than a predictable use of the prior art. In fact, given the clear differences between the content of both references when compared to the features of Appellants' claims, the combination of these two references clearly does not suggest Appellants' claimed invention.

For the above reasons, one skilled in the art would not find Appellants' invention unpatentable over the combination of references. The above example claims 5-7 and the corresponding dependent claims 13-16 and 21-24 are therefore allowable over the combination, and Examiner's rejection of these claims is not well founded and should be reversed.

CONCLUSION

Appellants have pointed out with specificity the manifest error in the Examiner's rejections and the claim language which renders the invention patentable over the primary reference and the combination of references. Appellants, therefore, respectfully request that this case be remanded to the Examiner with instructions to issue a Notice of Allowance for all pending claims.

Respectfully submitted,

/Eustace P. Isidore/

Eustace P. Isidore
Reg. No. 56,104
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANTS

APPENDIX

1.   A method in a data processing system for controlling the transfer of data from the data processing system to a network, said method comprising the steps of:

creating a file list of one or more data files to be controlled;

creating a process list for each data file in the file list, wherein each process list identifies one or more processes executing in the data processing system that has accessed the data file associated with the created process list;

receiving a request from a requesting process executing in the data processing system to transfer data from the data processing system to the network;

determining if the requesting process is identified in one or more created process lists; and

if the requesting process is identified in a created process list, prohibiting the requested transfer of data from the data processing system to the network.

2.   The method according to claim 1, wherein the step of creating a process list includes adding a first process to a process list when the first process receives data from a second process identified on the process list.

3.   The method according to claim 2, wherein the first process is only added to the process list when the received data is related to the process list's associated data file.

4.   The method according to claim 1, wherein the step of receiving includes receiving a request from a requesting process executing in the data processing system to transfer a data file listed in the file list from the data processing system to the network.

5.   The method according to claim 1, further comprising the step of requesting authorization to perform the requested transfer of data from the data processing system to the network.

6.   The method according to claim 5, wherein the step of requesting includes sending a message to a user of the data processing system displayed in a graphical user interface.

7.   The method according to claim 1, further comprising the step of performing the prohibited transfer of data from the data processing system to the network upon receipt of authorization to make the transfer of data.

8.   The method according to claim 7, wherein the authorization is a command received from a user of the data processing system.

9.   A data processing system for controlling the transfer of data from a data processing system to a network comprising:
        means for creating a file list of one or more data files to be controlled;
        means for creating a process list for each data file in the file list, wherein each process list identifies one or more processes executing in the data processing system that has accessed the data file associated with the created process list;
        means for receiving a request from a requesting process executing in the data processing system to transfer data from the data processing system to the network;
        means for determining if the requesting process is identified in one or more created process lists; and
        means for, if the requesting process is identified in a created process list, prohibiting the requested transfer of data from the data processing system to the network.

10.   The data processing system according to claim 9, wherein the means for creating a process list includes adding a first process to a process list when the first process receives data from a second process identified on the process list.

11.   The data processing system according to claim 10, wherein the first process is only added to the process list when the received data is related to the process list's associated data file.

12.   The data processing system according to claim 9, wherein the means for receiving includes receiving a request from a requesting process executing in the data processing system to transfer a data file listed in the file list from the data processing system to the network.

13.   The data processing system according to claim 9, further comprising means for requesting authorization to perform the requested transfer of data from the data processing system to the network.

14.   The data processing system according to claim 13, wherein the means for requesting includes sending a message to a user of the data processing system displayed in a graphical user interface.

15.   The data processing system according to claim 9, further comprising means for performing the prohibited transfer of data from the data processing system to the network upon receipt of authorization to make the transfer of data.

16.   The data processing system according to claim 15, wherein the authorization is a command received from a user of the data processing system.

17.   An article of manufacture comprising machine-readable medium including program logic embedded therein that causes control circuitry in a data processing system for controlling the transfer of data from a data processing system to a network to perform the steps of:

      creating a file list of one or more data files to be controlled;

      creating a process list for each data file in the file list, wherein each process list identifies one or more processes executing in the data processing system that has accessed the data file associated with the created process list;

      receiving a request from a requesting process executing in the data processing system to transfer data from the data processing system to the network;

      determining if the requesting process is identified in one or more created process lists; and

      if the requesting process is identified in a created process list, prohibiting the requested transfer of data from the data processing system to the network.

18.   The article of manufacture of Claim 17, wherein the step of creating a process list includes adding a first process to a process list when the first process receives data from a second process identified on the process list.

19.   The article of manufacture of Claim 18, wherein the first process is only added to the process list when the received data is related to the process list's associated data file.

20.   The article of manufacture of Claim 17, wherein the step of receiving includes receiving a request from a requesting process executing in the data processing system to transfer a data file listed in the file list from the data processing system to the network.

21.   The article of manufacture of Claim 17, further comprising the step of requesting authorization to perform the requested transfer of data from the data processing system to the network.

22.   The article of manufacture of Claim 21, wherein the step of requesting includes sending a message to a user of the data processing system displayed in a graphical user interface.

23.   The article of manufacture of Claim 17, further comprising the step of performing the prohibited transfer of data from the data processing system to the network upon receipt of authorization to make the transfer of data.

24.   The article of manufacture of Claim 23, wherein the authorization is a command received from a user of the data processing system.

EVIDENCE APPENDIX

Other than the Office Action(s) and reply(ies) already of record, no additional evidence has been entered by Appellants or the Examiner in the above-identified application which is relevant to this appeal.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings as described by 37 C.F.R. §41.37(c)(1)(x) known to Appellants, Appellants' legal representative, or assignee.